Office of the Saskatchewan Information and Privacy Commissioner January 2011

FOIP FOLI

INTERNATIONAL DATA PRIVACY DAY 2011

This Friday, January 28, 2011 is **International Data Privacy Day**. The theme in Canada this year is the slogan ***The Net Never Forgets. Remember To Protect Your Personal Data.***

To commemorate this year's event, the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) has a limited supply of 2011 privacy calendars available. The calendar features privacy cartoons and privacy tips. These calendars are available at our office located at 503 - 1801 Hamilton Street, Regina.

NEW PRIVACY FACES

The OIPC welcomes the following new staff who are filling existing vacancies for term positions.

Alyx Larocque joined the OIPC on December 29, 2010, as a Portfolio Officer. Alyx brings with her several years of experience from the Ministry of Social Services, including experience in the areas of child protection, foster care/resources, adoptions and most recently quality management.

Alyx holds a Bachelor of Arts degree majoring in psychology and a Bachelor of Social Work

(Continued on page 2)

INSIDE THIS ISSUE

International Data Privacy Day 2011.....1
New Privacy Faces.....1

SGI Privacy Report.....2
More Proactive Disclosure.....3

What Constitutes a Reasonable Search for a Record?.....3
Dismissal Deemed Appropriate for Snooping.....4

Can a Trustee Withhold from the Patient the Names of Care Providers?.....4
Let Me See Your Photo Collection so I can Determine Who to Sue.....5

Online Health Marketing.....5
Another SK Pharmacist Found to Have Violated HIPA.....5

Gmail Breaks Trail into Canadian Universities via University of Alberta.....6
Speaking of How Not to Respond to an Access Request.....6

Breach of PIPEDA can Cost Non Compliant Organizations Money.....6
Does FOIP Cover Personal E-mails Stored at Work?.....7

Freedom of Information and Privacy Association (FIPA) Developments.....7
Should your Family Doctor be using Social Networks to Communicate with Patients?.....7

Another Consideration for Trustees Contemplating Electronic Medical Records.....8
Ontario, the HST and the Burden of Proof.....8

Taking Photographs of Students at Schools.....9
Outsmart your Smart Phone.....9

Hunting for a Girlfriend on your Employer's Computer.....9
PIPEDA Amendment.....10

Mark your Calendar.....10

(Continued from page 1)

from the University of Regina. She is currently working towards her Master in Public Administration Public Management degree through the Johnson Shoyama Graduate School of Public Policy at the University of Regina.

We also welcome **Chantelle Probe** who started January 3, 2011 as a Portfolio Officer. Chantelle has worked in the Saskatchewan Government since 1998 following eight years experience as a business owner in Regina. Chantelle comes from the Ministry of Social Services where she worked predominately in the areas of access, privacy and security. She is currently completing her final course in the University of Alberta's Information Access and Protection of Privacy certificate program (IAPP).

SGI PRIVACY REPORT

In December the OIPC issued its Investigation Report F-2010-001 (SGI).

The OIPC received three formal 'breach of privacy' complaints that related to the collection, use and disclosure by Saskatchewan Government Insurance (SGI) of personal health information of claimants under *The Automobile Accident Insurance Act* (AAIA). The complaints alleged excessive collection of personal health information and improper use and disclosure of that personal health information.

Our office commenced formal investigations in respect to each of the three complaints. SGI took the position that there is a gap in Saskatchewan's legislative scheme for privacy protection. SGI asserted that the OIPC had no authority to investigate these matters since neither *The Health Information Protection Act* (HIPA) Parts II, IV and V, nor *The Freedom of Information and Protection of Privacy Act* (FOIP) applied to these complaints. The Commissioner considered representations from SGI and concluded that there is no evidence that the Legislative Assembly would have intended to create such a gap in legislated privacy protection and that, in fact, there is no such gap as alleged by SGI.

The OIPC has explored with SGI informal means to resolve the impasse but no such resolution appears possible.

The Commissioner recommended that the Legislative Assembly amend the appropriate legislation to clarify the rules that will apply to the personal information collected, used and disclosed by SGI in its activities under the AAIA and the role of the OIPC in overseeing SGI's statutory responsibilities under FOIP and HIPA. He also recommended that SGI publish on its website clear information about its collection, use and disclosure practices. He further recommended that SGI revise its procedure for collection of personal health information to ensure that it is not over-collecting such information. The full text of the Report is available at www.oipc.sk.ca under the *What's New* tab.

MORE PROACTIVE DISCLOSURE

The Department of National Defence (DND) has posted on its website requests for access to information that have been previously processed under the federal *Access to Information Act*. On the DND website a visitor will see the following notice under the Access and Privacy tab:

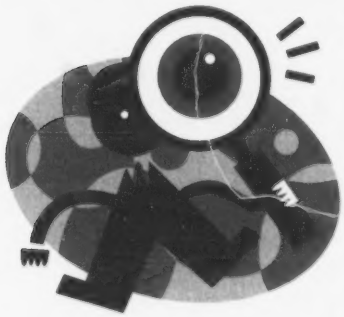
The following is a summary of Access to Information requests processed by the Department of National Defence. The list is not all-inclusive. Requests such as those that did not result in the release of any records or that contain primarily personal information of the original requester are not posted. The requests are displayed by the year and the month when they became available for public release. The records will be disclosed in the form that they were released under the Access to Information Act including format, language(s) and any exemptions or exclusions that were applied at the time of release.

If you wish to obtain a copy of the records released in response to these requests informally, you may write to us at the following address...

You can see the list and description of past access requests responded to by DND at http://www.admfincs.forces.gc.ca/aip/cr-dc-eng.asp.

Consider how useful that kind of step would be in this province. It would demonstrate to the public that a particular public body is committed to making FOIP work. It would allow requesters to determine what queries had already been made and would thus avoid duplication of requests and the work such duplicate requests would generate. If someone has made an access request for certain records, there is a very good chance that others would be interested in the same records. This development is very much aligned with the Open Government movement led by the cities of Toronto, Vancouver and Edmonton. What would be even more convenient for citizens would be a dedicated open government website on which there would be a list of all records released by any Ministry of the Saskatchewan Government, save for personal information.

WHAT CONSTITUTES A REASONABLE SEARCH FOR A RECORD?



Fundamental to a good access to information regime is an emphasis on public bodies undertaking an appropriately thorough search for records that are responsive to the request.

A December Order of the Alberta Information and Privacy Commissioner (IPC) addresses what a reasonable search looks like. Although Order P2010-010 was issued pursuant to Alberta's *Personal Information Protection Act* the Adjudicator relied on previous Orders under Alberta's FOIP Act in concluding that the organization in question failed to make a reasonable effort to search for the requested records. In general, evidence as to the adequacy of a search should cover the following points:

- Specific steps taken by the Organization to identify and locate responsive records
- Scope of the search conducted – for example: physical sites, program areas, specific databases, off-site storage areas, etc.
- Steps taken to identify and locate all possible repositories of records relevant to the access request: keyword searches, records retention and disposition schedules, etc.

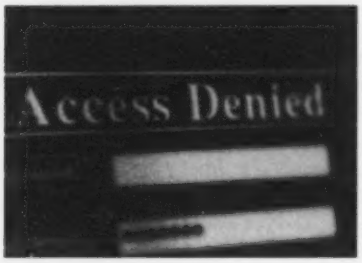
(Continued on page 4)

(Continued from page 3)

- Who did the search; and
- Why the Organization believes no more responsive records exist than what has been found or produced.

The full report is available at www.oipc.ab.ca. Saskatchewan FOIP Coordinators will also want to be familiar with the *Helpful Tips – Best Practices for Public Bodies/Trustees* sheet available at our website: www.oipc.sk.ca under the *Resources* tab.

DISMISSAL DEEMED APPROPRIATE FOR SNOOPING



Tuscon's University Medical Centre (UMC) fired three employees for accessing confidential medical records.

The records related to the shooting of U.S. Representative Gabrielle Giffords and 18 others on January 8, 2011. In a statement issued January 12, 2011 by the UMC:

"University Medical Center takes the privacy of all patients very seriously. The hospital has terminated three clinical support staff members this week for inappropriately accessing confidential electronic medical records, in accordance with UMC's zero tolerance policy on patient privacy violations. A contracted nurse also was terminated by the nurse's employer.

...With advances in technology, ensuring patient privacy has become the focus of hospitals nationwide. UMC uses sophisticated technology to help prevent and detect inappropriate access to patient information." You can access the full statement at http://www.azumc.com/

CAN A TRUSTEE WITHHOLD FROM THE PATIENT THE NAMES OF CARE PROVIDERS?

In Order H2010-003, an adjudicator in the Alberta IPC ordered Alberta Health Services (the Custodian) to disclose to an applicant his personal health information (phi) under that province's *Health Information Act*.

The custodian had provided the applicant with his health information, but in a few cases, withheld phi from the records, such as the names of some of the applicant's health service providers and treatment notes. The custodian did so on the basis that disclosing the information could reasonably be expected to threaten the mental or physical health or safety of individuals. The Adjudicator determined the custodian had not established that disclosing the applicant's health to him would pose a threat to the mental or physical health and safety of individuals.

You can read the full Order at www.oipc.ab.ca. Our office considered a similar claim in Reports H-2008-002 (Saskatoon Regional Health Authority) and H-2007-001(Saskatchewan Cancer Agency). A 'custodian' in Alberta is equivalent to a 'trustee' in Saskatchewan.

LET ME SEE YOUR PHOTO COLLECTION SO I CAN DETERMINE WHO TO SUE

The Ontario Superior Court of Justice recently dealt with an application by an individual who sought an order for pre-trial discovery.

The applicant was trying to identify the young female snowboarder who crashed into him while they were both on the ski hill causing significant injury to the applicant. This order would allow the applicant to view all of the membership photos of female members between 12 and 20 and to make copies. In law, what was sought was something described as a Norwich order.

Madam Justice Warkentin asked for additional submissions regarding the privacy rights of the female skiers whose privacy would be infringed by such an order. Justice Warkentin then denied the motion and found that as a matter of public policy, the government enacted PIPEDA "in order to protect and maintain the confidentiality of information that organizations have collected on all persons, not just of children." You can read the full Order at Douglas v. Loch Lomond Ski Area, 2010 ONSC 6483.

ONLINE HEALTH MARKETING

There is an interesting complaint submitted to the U.S. Federal Trade Commission by a number of agencies who allege that health marketers are violating Internet users' privacy by tracking their online activity to target them with ads "precisely honed to a particular illness or condition."

The 144 page complaint alleges that privacy is prejudiced by the practice of targeting medical or disease conditions and then tracking and digitally profiling a health concern of an individual. This activity raises concerns given the number of IT companies that are offering a range of patient portal type services to the Canadian public. This was contemplated by Canada's Information and Privacy Commissioners when they adopted their resolution in September 2009. You can read the resolution *The Promise of Personal Health Records* and backgrounder at www.oipc.sk.ca under the *What's New* tab.

ANOTHER SK PHARMACIST FOUND TO HAVE VIOLATED HIPA

The Saskatchewan College of Pharmacists, in its Volume 31 Number 2 Newsletter, reports that **Dan Kirkau** had been guilty of professional misconduct which included utilizing personal health information from a prescription database without consent and in breach of HIPA. Mr. Kirkau received a reprimand, a $5,000 fine and was ordered to pay costs of $9,000 failing which his license to practice shall be suspended. We dealt with another breach of HIPA by a pharmacist in our Investigation Report H-2010-001. This Report is available at www.oipc.sk.ca under the *Reports* tab.

GMAIL BREAKS TRAIL INTO CANADIAN UNIVERSITIES VIA UNIVERSITY OF ALBERTA

Google has entered the university market in Canada with the announcement in December 2010 that it has a contract with the University of Alberta (U of A) to replace the 30 different email systems formerly in use at the U of A with Gmail.

Google has undertaken by contract not to datamine Gmails from the U of A and not to share the data with a third party. The parties to the contract assert that the new arrangement is consistent with Alberta's FOIP Act.

SPEAKING OF HOW NOT TO RESPOND TO AN ACCESS REQUEST...

An example of what not to do when responding to an access request is provided by the Privacy Commissioner of Canada PIPEDA Case Summary 2010-003.

In this case an individual's initial request to access his personal information was ignored by the organization. His second request, several months later, required an extension to complete. He was not properly advised of the extension within the statutory time limits allowed by PIPEDA. He also permanently lost access to some of this personal information when it was deleted by the organization in accordance with its standard retention policies. Those policies did not take into account the time lag between the first and second access requests.

The Commissioner found that organizations should consider, and where necessary, override their regular deletion/retention practices until such time as the individual has exhausted any statutory remedies for access to that information. For the full case summary go to www.priv.gc.ca.

BREACH OF PIPEDA CAN COST NON COMPLIANT ORGANIZATIONS MONEY

It is commonly understood that businesses that are found by the Federal Privacy Commissioner to be non-compliant with PIPEDA will suffer a tarnished reputation. What must now also be considered as a consequence is a financial penalty assessed by the Federal Court.

In what is the first of its kind, the Federal Court, in a case involving TransUnion of Canada Inc., ordered TransUnion to pay the affected individual damages in the amount of $5,000.

In this case, TransUnion provided the individual's bank with a negative credit report that related to someone else with a similar name. It violated its duty to ensure accuracy by disclosing information to the bank that was "grossly inaccurate". TransUnion also failed to take adequate corrective action once it learned of the harm that resulted from its disclosure of inaccurate information. The citation for the decision of Nammo v. TransUnion of Canada Inc. is 2010 FC 1284.

DOES FOIP COVER PERSONAL E-MAILS STORED AT WORK?

An Ontario court case held that personal emails of a municipal solicitor, although stored on the city's email server, were not 'in the control' of the city.

In the result, the judge overturned an order of the Ontario IPC which had granted access to the applicant of the personal emails in question. You can read the decision of the Ontario Superior Court of Justice, Divisional Court at City of Ottawa v. Ontario, 2010 ONSC 6835. This decision has apparently been appealed.

For a recent discussion in Saskatchewan of what it means for a record to be *'in the possession or under the control of a local authority'*, see the OIPC Report LA-2010-002 (City of Saskatoon). This is available at our website: www.oipc.sk.ca under the *Reports* tab.

FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION (FIPA) DEVELOPMENTS

The British Columbia (BC) based Freedom of Information and Privacy Association (FIPA), in its December newsletter, welcomed new Executive Director **Vincent Gogolek**. Vincent has degrees in law and journalism and a diploma in International and Comparative politics from the London School of Economics. He succeeds the remarkable and tireless **Darrell Evans**. Darrell deserves a standing ovation for his leadership not only in BC but across Canada in promoting public sector accountability and transparency.

FIPA's impact on FOI in BC was clearly evident with the issue in December of an Order from BC IPC **Elizabeth Denham** directing the release of a complete copy of the $300 million Workplace Services Agreement with IBM. This process was triggered by an access request from FIPA six years ago. You can review the Order at www.oipc.bc.ca . You can also see the latest FIPA Bulletin at www.fipa.bc.ca.

SHOULD YOUR FAMILY DOCTOR BE USING SOCIAL NETWORKS TO COMMUNICATE WITH PATIENTS?

We note that the American Medical Association (AMA) has issued a new policy: *Professionalism in the Use of Social Media*. This lists a number of considerations physicians are to consider when maintaining a presence online. At the top of that list is the following:

> *Physicians should be cognizant of standards of patient privacy and confidentiality that must be maintained in all environments, including online, and must refrain from posting identifiable patient information online.*
>
> *When using the Internet for social networking, physicians should use privacy settings to safeguard personal information and content to the extent possible, but should realize that privacy settings are not absolute and that once on the Internet, content is likely there permanently. Thus, physicians should routinely monitor their own Internet presence to ensure that the personal and professional*

(Continued on page 8)

(Continued from page 7)

information on their own web sites and, to the extent possible, content posted about them by others, is accurate and appropriate.

Saskatchewan physicians will be mindful that HIPA and key provisions such as section 16 are technology neutral in that they apply to personal health information in the custody or control of trustees such as physicians in any and all technological applications including social networks. We understand that neither the Canadian Medial Association (CMA) or the Saskatchewan Medical Association (SMA) have a specific policy dealing with social networking. Trustees, however, are encouraged to become familiar with CMA policy for physician guidelines for online communication with patients. This is available at www.cma.ca.

ANOTHER CONSIDERATION FOR TRUSTEES CONTEMPLATING ELECTRONIC MEDICAL RECORDS

As more and more Saskatchewan physicians consider converting to an electronic medical record system for their patient information, they would do well to make sure they consider how they and the provider will manage the end of the relationship. Is there a clear and compliant exit strategy when the relationship with a vendor ends? There should be a positive obligation on the provider to act in good faith to facilitate a smooth transition to a new provider. It is also important to ensure an adequate indemnity provision as well as clear language that addresses responsibility for the collection/creation of personal health information as well as use of that phi.

ONTARIO, THE HARMONIZED SALES TAX (HST) AND THE BURDEN OF PROOF

For FOIP Coordinators preparing a submission to an Information and Privacy Commissioner, a timely reminder about the importance of the burden of proof is a feature of the recent Order PO-2919 (Ministry of Finance) issued by the Ontario IPC on October 14, 2010.

With a number of the exemptions claimed by the public body and considered by the IPC, the IPC found insufficient evidence to sustain the exemptions claimed. For example, in denying the exemption claimed for "economic and other interests" the IPC stated that "Parties should not assume that harms under section 18 are self-evident or can be substantiated by submissions that repeat the words of the Act". The IPC also found insufficient evidence to meet the burden of proof for the 'cabinet records', 'policy options or recommendations', 'consultations among ministers', 'advice to government' and 'relations with other governments' exemptions. We recommend this Order to all new Saskatchewan FOIP Coordinators. You can read this Order at www.ipc.on.ca.

DATA PRIVACY DAY IS JANUARY 28, 2011

TAKING PHOTOGRAPHS OF STUDENTS AT SCHOOLS

Our office often receives calls from school officials and occasionally parents seeking information about photographs taken in schools. A very useful resource published by the Alberta OIPC has some good advice for schools in our province too. You can access the *Information Bulletin – Taking Photographs of Students at Schools* at www.oipc.ab.ca.

OUTSMART YOUR SMART PHONE

In a timely caution, **Jennifer Stoddart**, Privacy Commissioner of Canada, reminded Canadians that smart phones and their mobile apps are appealing but they also have an appetite for your personal information.

Commissioner Stoddart noted that *"A fully-loaded smart phone is like carrying around a tiny little communications satellite, bristling with sensors and antennas. It's constantly sending and receiving data about your activities and your whereabouts. But where is the data going? What is it saying about you? And what is the effect on your privacy."*

Commissioner Stoddart offered the following tips for smarter phone use including:

- Do your due diligence
- Think it through
- Keep it safe

For more information, visit www.priv.gc.ca.

HUNTING FOR A GIRLFRIEND ON YOUR EMPLOYER'S COMPUTER

A fellow who worked for the Social Security Administration in Florida used his work computer to collect personal information (pi) about women he knew.

The employee was sentenced to 12 months in jail after being convicted of violating the federal *Computer Fraud and Abuse Act*. Significantly, the court stated: "his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access." [emphasis added]

The employee had argued that he had not obtained the pi for any criminal purpose and that he did this so he could send gifts, flowers and birthday cards to these women although they had not given him their addresses or dates of birth.

PIPEDA AMENDMENT

Please note that PIPEDA has been amended to prohibit the collection of pi by means of unauthorized access computer systems and the unauthorized compiling of lists of electronic addresses. This was effected by c. 23 S.C. 2010 otherwise concisely known as *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-Television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act.*

And you wondered why there are so many acronyms in access and privacy practice!!

MARK YOUR CALENDAR!

Canadian Bar Association Privacy and Access Law Section meetings in Regina and Saskatoon. To register for any of the following section meetings call CBA at (306) 244-3898.

REGINA

February 14, 2011: *Privacy and Access Law Section South*, Hotel Saskatchewan, Regina at 12:00 noon. Topic: Breach Notification, Speaker: Gary Dickson, Q.C., Saskatchewan Information and Privacy Commissioner

SASKATOON

February 15, 2011: *Joint Administrative and Labour Law North and Privacy and Access Law North,* Saskatoon Club, Saskatoon at 12:00 noon. Topic: Privacy Issues in Employment, Speaker: Gary Dickson, Q.C., Saskatchewan Information and Privacy Commissioner

January 28, 2011: Data Privacy Day Session 2011— *Do you believe your privacy is protected in the...Health sector, Public sector and Private sector?* Delta Edmonton Centre Suite Hotel—Conference Centre, Edmonton, Alberta. For more information visit Data Privacy Day Session 2011.

February 16—18, 2011: 12th Annual Privacy and Security Conference—*Security and Privacy—Is there an app for that?* Victoria Conference Centre, Victoria, British Columbia. For more information visit www.rebootconference.com/privacy2011/

March 10—11, 2011: 2011 Information Management, Access, Privacy Symposium. Metro Toronto Convention Centre, South Building. For more information visit www.imaps2011.ca

OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER

503 – 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Telephone: (306) 787-8350 / Toll Free: 1-877-748-2298 / Fax: (306) 798-1603
E-mail: webmaster@oipc.sk.ca Website: www.oipc.sk.ca

If you wish to subscribe to the Saskatchewan FOIP FOLIO, please send your e-mail address to webmaster@oipc.sk.ca.